DID + DPKI + Mobile Number + Identity Ecosystems + Global Services

Introduction

UID-NUM is a Decentralised Identifier (DID) project based on access to a unique non-country specific Universal Personal Telecommunications dialing code (+878.10) providing the capacity to allocate, using decentralised nodes, up to 10 billion 15-digit mobile phone numbers to support an ecosystem of numeric identifiers for individuals.

UID-NUM uniquely combines mobile connectivity across a global number range with PKI cryptography on SIM cards to create and support number based self-sovereign identity and credential verification platforms and ecosystems which enable secure applications for remote transactions without correlating traceability or creating ‘super-cookies’.

The UID-NUM ecosystem is user-centric and provides individuals with lifetime ownership and complete control of a DID with three levels of self-generated pseudonymic numbers and the flexibility to adjust the level of pseudonym number exposure to the required level of data disclosure and credential verification.

UID-NUM’s 3 level DID

The three levels of a UID-NUM DID combine to create an open interoperable ecosystem providing an individual with the ability to generate a cryptographic realm of rotating numbers and manage them conveniently from an identity wallet mobile interface. The individual’s ability to use the appropriate level of UID-NUM DID means disclosures can be limited to essential information only and they do not need to provide a full range of personal data when a counter-party only requires one minor piece.

The first two levels of UID-NUM numbers are not telecom numbers but PKI rotating numbers in an easy-to-read format for presentation to a counterparty instead of name and surname.

DID Level 1 – A ‘raw’ self-generated credential number not linked to any personal data but embedded with pairwise Decentralised Public Key Infrastructure (DPKI) to enable the individual to prove their link to the number cryptographically without revealing their name or any other any identifying data.

DID Level 2 – Enables an individual to self-generate an infinite range of cryptographic numbers as a ’backed pseudonym’ identity that does not reveal their name but allows them to verify specific pieces of personal information to a counterparty. For example, that the owner of the credential number is over 18 and that they are a citizen of a particular country.

DID Level 3 – This level of UID-NUM supports the two lower levels and comprises a ’real me’ UID-NUM comprising a global mobile phone number with the format +878.10 57.98.02.76.33 linked to a PKI enabled SIM card which does not itself disclose the individual’s identity to the recipient but enables the individual to reveal it if necessary together with the ability to authorise the counterparty to verify any other key pieces of personal information which they may require for the particular event. A 'real me' UID-NUM could even be used to digitally sign a legally binding contract in place of the individual's name.

An individual can own several UID-NUM identities of each level for use across a range of data sets and digital identity ecosystems, managing a suite of DIDs and personal data silos without traceability or correlation due to the use of self-generated rotating numbers instead of personal data (e.g. name and address) as the identifier.

Further details are set out in Appendix 2, the UID-NUM High Level Roadmap.

How UID-NUM benefits the Individual

UID-NUM provides a unique and user-centric method for an individual to acquire lifetime ownership of a DID verifiable through DPKI cryptography combined with SIM card connectivity for secure digital mobile interaction enabling the DID to be used for trusted identity and credential verification without exposure of name or other personal data and without correlated traceability.

As lifetime owner of a DID acquired from the UID-NUM node network it is the individual, rather than the mobile network operator, who controls the mobile phone number making it provider-agnostic and portable across mobile networks and digital identity ecosystems. When provisioned on a mobile network a UID-NUM DID enables a range of bio-metric methods to be implemented as an additional security level of identity verification. Details of how a UID-NUM mobile number interacts with a mobile network operator are set out in Appendix 1.

A UID-NUM identity could enable an individual to take advantage of the trusted image, range of services and global reach of a commercial brand operating within a digital identity ecosystem.

UID-NUM supports the concept of "encrypted personal databox tagging" with the individuals legally defined and mathematically ensured property rights over the contents of the tagged databox. The box is tagged by a UID-NUM number without exposing user's name and surname but with the ability to access them where necessary securely and legally.

How UID-NUM interacts with Identity Ecosystems

The UID-NUM project aligns the key W3C requirements for a unique individual identifier with the cryptographic and global mobile telephony capabilities of the +878.10 number range.

UID-NUM has been architected to play a core role as a 'raw' foundation DID with the ability to be embedded within multi-stakeholder global ecosystems of trusted digital identity and credential verification. UID-NUM features the ability:

- to be readable, memorable, writeable and pronounceable for humans while at the same time being natural for machines;
- to be embedded within the multi-stakeholder global ecosystems of trusted digital identity and credential verification envisaged by corporations such as Mastercard and Microsoft;

- to facilitate trusted interaction in any environment for the end-user by providing access to a range of sophisticated financial and other identity dependent services and equally in remote human-to-human transactions or in person, even in under-digitalised parts of the world.

Commercial brands providing services to individuals across the globe could use their trusted image to collaborate with UID-NUM in the provision of a DID and unique credential verification function.

UID-NUM's range of up to 10 billion DIDs can be made available to organisations for decentralised allocation to a global community of individuals through a branded app or internet interface and, in collaboration with MNOs and SIM card manufacturers, decentralised provisioning on mobile networks.

The UID-NUM concept is architected to engage mobile operators as key partners and offers significant commercial benefits but is not dependent on adoption by all mobile operators'.

Invitation to collaborate

UID-NUM has used its access to a unique number range to develop a decentralised privacy-enhancing DID framework which is secure, smart, simple and fully inter-operable with the emerging multi-stakeholder ecosystems providing trusted and decentralised identity and verification.

Using its mobile telecommunications expertise, the UID-NUM team will collaborate with partners in the development of an integrated system for mobile number management and network routing within a decentralised identity authentication environment.

UID-NUM invites expressions of interest from global corporations, financial institutions, SIM card manufacturers, mobile network operators, governments, NGOs and any other organisations interested in powering the global digital interactions of the future.

Further information

Further details of the UID-NUM project can be found in these Appendices.
Appendix 1 – Managing a UID-NUM mobile number
Appendix 2 –High level Roadmap

APPENDIX 1

Managing a UID-NUM mobile number

Managing numbers in a fully decentralised way means that every number is received by its owner not from a mobile service provider but directly, via DLT.

When the end-user immutably acquires a “real-me” UID-NUM mobile number (like +878.10.67.23.44.01.74) for the first time, he presents DID credentials sufficient for the mobile operator to activate the mobile subscriber with a cryptographic SIM card according to his country’s telecom regulations. The mobile operator learns the real name, surname and other relevant data of the person but they are not placed on DLT. On DLT, a record is created like “I, Mobile Operator X, know the real person who owns +878.10.67.23.44.01.74 and I now host this number on my network.” Most countries’ telecom regulations require that operator knows its subscribers, similar to banking regulations, under the KYC rules. These regulated entities keep the knowledge of their customers as their most valuable secrets. Even if someone hacks the operator’s subscriber database and learns which person has what “real-me” UID-NUM mobile number this knowledge has no value for the hacker.

If the end-user decides to swap his mobile operator or port his UID-NUM to another operator’s SIM card then he can do it without asking his current operator. He simply generates a record like “I, owner of +878.10.67.23.44.01.74, withdraw my number +878.10.67.23.44.01.74 from being hosted anywhere.” and then he goes to Operator Y of his choice, who supports UID-NUM, and they together generate a new record “I, Operator Y, know the real person who owns +878.10.67.23.44.01.74 and I now host this number on my network.” If the end-user does not need a PKI SIM-card in his phone but still wants to use UID-NUM telecom functionality (addressing messages to +878.10), he may choose a compliant broadband operator and have PKI signature generated on another type of device or cloud.

APPENDIX 2

UID-NUM's High-Level Roadmap

Step 1 - Develop a DLT network of decentralised nodes from which individuals can acquire immutable lifetime ownership of any quantity of tokenised 15-digit numeric Decentralised Identifiers (DID) embedded with pairwise Decentralised Public Key Infrastructure (DPKI) to prove ownership of the DID numbers and enable the individual to assert cryptographically "I am 814.08.17.67.11.35.34" without any personal data linked to this decentrally generated number.

Step 2 – Enable the individual, having any numeric DID of the above format, to immutably obtain ownership of a 15-digit numeric decentralised global mobile phone number of the "real-me" format (+878.10.67.23.44.01.74) without putting any personal data onto the blockchain. This "real-me" telecom number is generated with the provisioning to a real person that demonstrates their decentralised credentials, including name and surname, to a mobile network operator and a bank or similar institution that become the trust providers with the ability to confirm knowing the individual to a third-party without exposing the individual's name. The "real-me" global mobile number provisioned with a mobile network operator of the user's choice on a national SIM card with PKI cryptographic signature function, alongside with national mobile number, will serve only for messaging interaction within trusted ecosystems providing verification of their digital identity and credentials for mobile phone based transactions; they will not be used for voice calls or any other telecommunication services.

The individual will be the only person deciding on the provisioning mobile network for the number. He/she will be able to take the "real-me" number with him/her unilaterally without needing the mobile operator's or the consent of a bank or other trust provider. He/she will be able to keep the once generated "real-me" number even not provisioned to any mobile network.

Step 3 – Enable the individual with the "real-me" number to generate any quantity of "backed pseudonym" numbers as decentralised credentials and to manage them efficiently in a "personal DID realm" with the help of DID infrastructure and enable the individual to assert cryptographically "I am 814.08.17.67.11.35.34 and there are trusted third parties who have verified my real identity and will disclose it to you under the defined procedures."

Step 4 – Enable any two parties, having UID-NUM numbers of corresponding grades, to set an "encrypted tagged personal databox", to tag it with their UID-NUMs in a DID manner so that trust goes both ways and to sign a legally binding agreement defining property rights and usage authorisations/permissions for the content of the box;. The parties will then place digital credentials or data fragments into that box, dynamically changing the box contents and migrating data between such encrypted tagged databoxes.